La Administración se marca como objetivo aumentar la seguridad de sus datos

Publicado el **03/06/2008**, por **Expansión**

Ataques de 'hackers' o web con puertos abiertos son algunos de los defectos presentes en las páginas de Internet de las instituciones públicas. Todas las administraciones han apostado por las nuevas herramientas de protección.

La seguridad de los sistemas de la Administración pública es una de las preocupaciones del Gobierno, debido a la sensibilidad de los datos que incluyen sus archivos, (declaración de la renta o pagos a Hacienda), que requieren un mayor control. Para la labor de protección de los datos, en 2004 se creó el Centro Criptográfico Nacional (CCN), un organismo que ha realizado distintos proyectos de seguridad en la red de las instituciones públicas. Entre ellos figura el programa Respuesta ante Incidentes de Seguridad de la Información (CCN-Cert), destinado a todas las Administraciones del Estado.

Los piratas informáticos o hackers, virus, phising, gusanos, troyanos, malware, spyware, pharming,..., todos los peligros que acechan en la red no son ajenos a la Administración pública. Por ejemplo, muchas instituciones de distintos países ha sufrido ataques de hackers que han modificado sus páginas en Internet.

Según los responsables del CCN, dependiente del Centro Nacional de Inteligencia (CNI), entre 2004 y 2006 estas amenazas crecieron un 55%, aunque de las detectadas cada ejercicio (2.057 en 2006) sólo se materializó una cuarta parte de media. El peligro no es sólo numérico, cada vez los ataques cibernéticos son más graves. "Antes esas técnicas de ataque estaban en manos de especialistas, ahora están pasando al gran público, a todo el mundo", admite Luis Jiménez, director adjunto del Centro Criptográfico Nacional.

Respuesta
La capacidad de respuesta del proyecto ante incidentes de seguridad en la información se concentra en todas las administraciones del Estado, central, autonómica y local. Entre sus funciones estarán la formación de personal especializado, la difusión de alertas, técnicas de detección y desactivación de amenazas.

Además, con este plan se establecerán cauces de comunicación e intercambio de experiencias con los dos centros que coordinan este proyecto la Universidad Politécnica de Cataluña y el de la Red Iris (comunidad académica y de investigación gestionada por Red.es).

Una de las soluciones para mejorar la seguridad también ha sido la unión entre administraciones. En 2007, el Instituto Nacional de Tecnologías de la Información (Inteco) y el Centro Criptográfico Nacional firmaron un acuerdo para impulsar los aspectos de seguridad en las nuevas tecnologías de la información. Dentro de los puntos principales de este acuerdo se encuentran los requisitos de seguridad de las aplicaciones que empleen el nuevo DNI electrónico. Además, con este acuerdo se ha potenciado el intercambio de información, la formación especializada y el desarrollo de proyectos.

Con este acuerdo, el Gobierno pretende fijar las bases de colaboración para impulsar en España la seguridad dentro del desarrollo de la Sociedad de la Información. ¿Cómo piensa hacerlo la Administración? Por medio del intercambio de información, la formación especializada y el desarrollo de proyectos tecnológicos.

Importancia
En la presentación del acuerdo, el subdirector general adjunto del Centro Criptográfico Nacional, Luis Jiménez, y el director general del Inteco, Enrique Martínez, manifestaron la importancia de estos acuerdos para la implantación segura de la sociedad de la información.

Para Jiménez, las instituciones públicas no puede ser ajenas a estas tecnologías, “pero con la necesidad de que la elaboración, conservación y utilización de determinada información se realice de forma segura para garantizar su funcionamiento eficaz”.
Por otro lado, desde 2004, el Gobierno español a través del Centro Nacional de Inteligencia (CNI), mantiene un acuerdo con el grupo estadounidense Microsoft para acceder al código fuente de Windows para proteger sus sistemas. Esta compañía ha desarrollado el Programa de Seguridad para Gobiernos (GSP) con el que se proporcionan a las administraciones e instituciones públicas información técnica para localizar errores o herramientas criptográficas.

“Tanto la evaluación como la certificación de la integridad son tareas complejas y no pueden iniciarse sin conocer completamente cómo está constituido el hardware y el software del producto. Con ello se puede evaluar los mecanismos de seguridad de un producto para la posterior verificación de su integridad”, declaró Jorge Dezcallar, en ese momento director del CNI, en la presentación del acuerdo.
Otro de los puntos polémicos es el nuevo reglamento que afectará a los datos personales. Desde abril de este año, la Ley Orgánica de Protección de Datos (Lopd) se encarga de regular este aspecto, aclarando puntos fundamentales para la protección de datos tanto en la Administración como en el mundo empresarial.

Nueva norma
Mantener un documento de seguridad o aclarar que se entiende por ficheros relacionados con actividades personales o domésticas son algunos de los puntos que modifica esta nueva ley.

Según Julio Pérez, secretario de Estado de Justicia “esta norma dota de mayor grado de certeza, lo hace más previsible e incrementa la seguridad jurídica. Establece mecanismos concretos de ordenación de los derechos subjetivos”.
A nivel local, la presencia de las nuevas tecnologías también ha crecido entre los ayuntamientos. Según un estudio de Inteco, el 80% de los consistorios pequeños o medianos tienen ya acceso a Internet.

Entre las principales herramientas de seguridad destaca los antivirus, que lo utilizan el 98% de los consistorios, y los cortafuegos con un 70%. Para Inteco la implantación de las principales medidas de seguridad muestra un índice medio del 50% en los ayuntamientos. Sin embargo, estás herramientas son las únicas con las que cuentan la mayoría de las administraciones locales para su seguridad y, en muchos casos, son insuficientes. Para solucionar problemas como el spam (correo basura), sólo el 70% de ayuntamientos cuentan con un programa específico.

Diferencias
Dentro del estudio destaca el diferente nivel de seguridad entre los grandes municipios y los medianos o pequeños. Por ejemplo, el acceso a una red a través de una clave de seguridad se encuentra tan sólo en el 60% de los ayuntamientos con poca población. Mientras las ciudades registran un 70% de redes con un acceso con contraseña.

En sus conclusiones, Inteco recomienda a los consistorios la certificación de su seguridad, junto con la instalación de las firmas digitales, que sería un complemento a las actuales medidas de seguridad.

Por todo ello, el subdirector general adjunto del Centro Criptográfico Nacional, Luis Jiménez, piensa que “la Administración debe dotarse de los medios adecuados para la protección y control del acceso. Debe contar con unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión de la información”, concluye.